Notice of Allowability	Application No. 09/622,371	Applicant(s) MIYAZAKI ET AL.	
	Examiner Minh Dieu Nguyen	Art Unit 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *Amendment dated 6/10/2004*.

2. ☒ The allowed claim(s) is/are *3-5 and 8-19*.

3. ☒ The drawings filed on *10 June 2004* are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date June 10, 2004
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

Allowable Subject Matter

1. The amendment dated June 10, 2004 from the applicant has been entered and fully considered.

The amendment includes the amended claims 3-5 and 8-9, the cancelled claims 1-2 and 6-7 and the added claims 10-19.

2. The following is an examiner's statement of reasons for allowance:

The present invention is directed to provide means and technique for disabling secret information in a secure cryptographic device and invalidating an attacking method such as timing attack, differential power analysis, simple power analysis to a secure cryptographic device as an IC card.

The closest prior arts, Ishii (5,768,389), Liskov et al. (6,411,715) and Scheidt et al. (2002/0080970) fail to teach storing circuit in the secret information processing apparatus further has converting means for converting the secret information forming information into another secret information forming information and said another secret information forming information is information for allowing the secret information forming information processing means to output the same processing result (claims 3 and 8); apparatus on a receiver side of the processing result has means for setting the secret information forming information processing means and the secret information forming information into the storing circuit of the processing apparatus and an apparatus on a user side of the processing apparatus comprises means for inputting the data serving as a

processing target to the processing apparatus, means for receiving the processing result from the processing apparatus and means for transmitting the received processing result to the receiver side apparatus (claim 9) and arithmetic operation processing circuit comprises conversion means for converting the secret information forming information to other secret information forming information having relationship with regard to the secret information and used to form the secret information and processing means for executing a step of calculating a latest intermediate data for one or a plurality of times and a step of calculating a processing result by using the latest intermediate data wherein the step of calculating the latest intermediate data comprises a step of calculating the latest intermediate data different from the secret information by using a processing target, the other secret information forming information and initial data and a step for replacing the initial data by the calculated latest intermediate data (claim 12).

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

3. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 703-305-9727. The examiner can normally be reached on M-F 6:00-2:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on 703-306-3036. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Minh Dieu Nguyen
Examiner
Art Unit 2137

mdn

Andrew Caldwell
Andrew Caldwell